AFFIDAVIT

I, Dan Grossenbach, Postal Inspector for the United States Postal Inspection Service, being duly sworn, declare and state as follows:

INTRODUCTION

1. Based on the information in this affidavit, I believe there is probable cause that the following Defendant Cryptocurrencies were involved in a transaction or attempted transactions in violation of 18 U.S.C. §§1956 and 1957 (Money Laundering), and which constitute or were derived from proceeds traceable to violations of 18 U.S.C. §1343, and are therefore subject to forfeiture pursuant to 18 U.S.C. §§981(a)(1)(A) and (a)(1)(C).

Seized from Binance user ID 36412394:

Currency Name	Currency Code	Amount
USDT	TetherUS	46,990
USDT	TetherUS	63,850

Seized from Binance user ID 362242577:

Currency Name	Currency Code	Amount
BNB	BNB	9.9990
BTTC	BitTorrent	319,112,718
SHIB	SHIBA INU	102,070,628.68
FTM	Fantom	1,253.602517
ETH	Ethereum	3.998335
USDT	TetherUS	145,400.1033
MTH	Monetha	305,871.433
DOGE	Dogecoin	45,838.48318

Seized from Binance user ID 63916663:

Currency Name	Currency Code	Amount
BTC	Bitcoin	2.83040268
ETC	Ethereum Classic	77.72361915

BACKGROUND OF AFFIANT

2. I am a U.S. Postal Inspector tasked with investigating crimes related to the U.S. Postal Service. I have been employed by the U.S. Postal Inspection Service ("USPIS") since July 2004 and I am currently assigned to the Phoenix Division in Tucson, Arizona where I also serve as a Task Force Officer on the FBI's Southern Arizona Elder Fraud Task Force. I completed a bachelor's degree in criminal justice from the University of Arizona, a master's degree from Biola University, a 12½ -week training academy, and numerous other related training programs. I currently serve as adjunct faculty in the School of Government and Public Policy at the University of Arizona in Tucson. I have written and executed over one-hundred search warrants including seizure orders of financial currencies or assets in elder exploitation cases. I have personal experience with crypto currency which I've traded on platforms of four different exchanges and have held assets on both hot and cold storage wallets. I also keep current by listening to recent podcasts and reading books published on the topic of cryptocurrency.

3. As a Postal Inspector I have received significant training on how people use computers to commit crimes and the law enforcement techniques that can be utilized to

investigate and disrupt such activity. I have also been involved in, among other things, online and in-person undercover operations, as well as controlled drug deliveries and transactions. Moreover, in the course of my investigations and other cases on which I have worked, I have gained experience executing search warrants for physical premises, as well as for electronic evidence and data, including the content and other data associated with email, messenger, financial, and digital-marketplace accounts operating on both the traditional Internet and the dark web (as that term is defined below).

4. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

FACTS

7. I investigated a tech support refund scam perpetrated on 82-year old Tucson, Arizona resident D.M. My investigation showed that starting on February 23, 2022, and continuing through February 28, 2022, D.M. was defrauded of approximately $1.67 million by an unknown party(ies) in a tech support refund scam. The investigation was able to trace some of D.M.'s funds to Binance accounts, and some of those funds were seized pursuant to seizure warrants issued by Magistrate Judges in Tucson, Arizona.

8. On February 23, 2022, D.M. received an email claiming to offer a $190 refund from McAfee antivirus software. When D.M. called the phone number on the email to claim the refund, the person on the phone (SUSPECT #1) gave him a series of instructions which he followed. One of the instructions was to install a remote viewing software program which allowed SUSPECT #1 to control D.M.'s computer and manipulate the images on the screen. D.M. was not aware he was giving access to his computer but believed that this was a necessary step in processing his refund. SUSPECT #1 told D.M. that the refund was processed and deposited into D.M.'s bank account but that he (SUSPECT #1) erroneously deposited $500,000 into D.M.'s account instead of $190. D.M. believed he could see the transaction on his screen but only later realized that it was a false image displayed by SUSPECT #1 who had control of D.M.'s computer.

9. SUSPECT #1 urged D.M. to follow more instructions to correct the error and pay, what D.M. was falsely led to believe, was the return of a significant overpaid refund amount. Through the course of several interactions over the following four days, SUSPECT #1 continued regular telephonic contact to successfully obtain D.M.'s personal and financial information along with access to his computer and email accounts.

10. D.M. reported that his Gmail account was accessed without his authorization and the email correspondence to and from the suspects were deleted. A copy of a Gmail access log for D.M.'s Gmail account shows sign-on/account access history-originating from "West Bengal, India" on February 24, 2022, at 10:58 a.m. This was the same day D.M. reported speaking with SUSPECT #1.

11. On February 27, 2022, D.M.'s son called him as part of a routine check-up with his father. When D.M. described what was happening, his son told him it sounded like a scam. D.M. then shut down his computer and contacted his financial institution, Charles Schwab. A representative at Charles Schwab confirmed unauthorized withdrawals of approximately $2.2 million in assets and was able to stop one transfer of approximately $500,000 of that amount. The total amount of withdrawals was approximately $1.67 million.

12. During D.M.'s interactions with SUPSECT #1, a cryptocurrency account in D.M.'s name was opened with an exchange called "OK Coin." SUSPECT #1 told D.M. this was the only way to repay the $500,000 overpayment that D.M. falsely believed he owed. D.M. knew that the only account he owned that had enough money in it to cover the perceived overpayment was his Charles Schwab retirement account. Therefore, D.M. gave SUSPECT #1 his Charles Schwab account information and placed calls to Charles Schwab to authorize wires. However, D.M. became confused and was unaware of the exact amount of funds being withdrawn.

13. While there are thousands of different cryptocurrencies on the blockchain, all of the transactions referenced in this report involved the USDT token. This token is also known as "Tether" as it is generally tied to the value of the United States dollar.

14. Since the USDT token is tied to the value of the dollar, it is generally considered a stable means of conducting financial transactions. This feature combined with the anonymity involved in virtual currency makes it a common token used by criminals to launder proceeds from illegal activity.

15. On February 23, 2022, SUSPECT #1 established a new bank account in D.M.'s name at Signature Bank. SUSPECT #1 moved funds from D.M.'s Charles Schwab account to Signature Bank.

16. On February 24, 2022, SUSPECT #1 opened an account at cryptocurrency exchange OK Coin which was funded by the account set up the prior day at Signature Bank. After funds were moved from D.M.'s Charles Schwab account to Signature Bank, the account at Signature Bank was linked to the OK Coin exchange account. Those funds were then used to purchase 1,669,436 USDT on the exchange in the following transactions:

a. 02/24/22 500,000 USDT

b. 02/24/22 500,000 USDT

c. 02/26/22 669,436 USDT

17. The movement of cryptocurrency funds after this point was traced by an FBI Forensic Accountant (FA). Cryptocurrency transactions are visible as open source data on the internet. Through specialized training and experience along with tools available to law enforcement, the FBI FA was able to trace some of the proceeds stolen from D.M. through available blockchain records. My affidavit does not account for all of his analysis and some transactions were not able to be traced. However, the FBI FA was able to trace proceeds stolen from D.M. to four wallets. Only the funds in two wallets (TWXd wallet and TPQ2 wallet)

transferred to Binance accounts.[1] The data and summary chart below, which describe the movement of these virtual funds, are a result of the FBI FA's analysis.

18. Between February 25, 2022, and February 26, 2022, withdrawals from the OK Coin account, that had been fraudulently funded with D.M.'s Charles Schwab funds, were made in four separate transactions totaling 1,669,436 USDT going to four separate virtual wallets as follows: (1) on February 25, 2022, TPQ2iafQDsyVGMKsjV1MB8oN2 ("TPQ2") received 494,623 USDT; (2) on February 25, 2022, TWXdg24HGmAooXP97pKtgyhycKrH7JJ12P ("TWXd") received 492,159 USDT; (3) on February 26, 2022, TBAFzujUPcv1TA4keA8p9aUnSJNhAStPEA ("TBAF") received 182,654 USDT; and (4) on February 26, 2022, TTSq2ytNLP8ywXL22tZDmDmtxr3T4rne6K ("TTSq") received 500,000 USDT. (See Chart 1, below.)

19. Tracing the funds that went into the third and fourth wallets described above, TBAF and TTSq, was not feasible. The analysis described below, follows the first two transactions conducted on February 25, 2022, involving the first and second wallets described above, TPQ2 and TWXd.

20. On February 25, 2022, all 492,159 USDT in TWXd was sent from TWXd to TPQ2. This left wallet TWXd depleted of funds and resulted in a total of 986,782 USDT of D.M.'s money now consolidated in TPQ2. (See Chart 1, below.)

[1] The remaining funds that went into the TBAF and TTSq wallets described below were then split into multiple transactions and traced to multiple other wallets owned by other unknown individuals. Further tracing is not feasible.

21. Between February 26, 2022, and February 28, 2022, the funds in the now-consolidated TPQ2 wallet was sent to five different wallet addresses. Of those five new wallets, the FBI FA was unable to trace 219,782 USDT that went into three wallets. However, the FBI FA was able to trace a total of 767,000 USDT to two (2) wallets on the cryptocurrency exchange Binance, as follows:

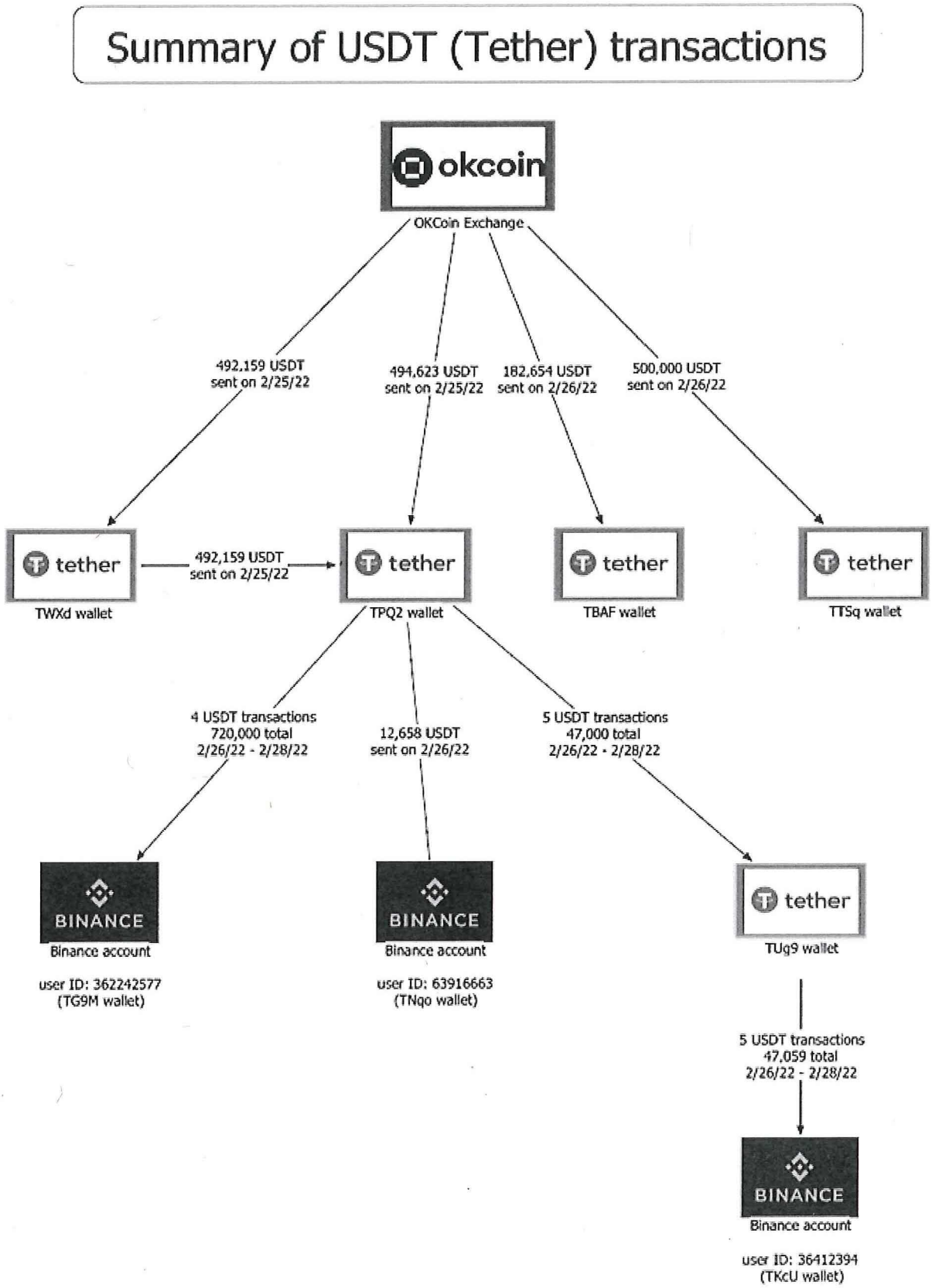
a. Binance User ID 362242577: Between February 26, 2022, and February 28, 2022, four separate transactions, totaling 720,000 USDT was sent from wallet TPQ2 to wallet TG9M on the Binance exchange, which was identified by Binance as the deposit address for account held by Indian citizen R[redacted] R[redacted] (hereinafter "R.R.") (See Chart 1, below.)

b. Binance User ID 63916663: On February 26, 2022, one transfer of 12,658 USDT was sent from wallet TPQ2 to wallet TNqonJMEhRV5m6AFQXQbiekhyUHs94p1Q6 [TNqo] on the Binance exchange, which was identified by Binance as the deposit address for account held by India citizen R[redacted] S[redacted]. (hereinafter "R.S.") (See Chart 1 below).

c. Binance User ID 36412394: Between February 26, 2022, and February 28, 2022, five separate transactions, totaling 47,000 USDT was sent from wallet TPQ2 to wallet TUg9Yu4sZwzV8SYqBc3np8SmvYwKm1mNKT [TUg9]. This wallet was later identified as belonging to India citizen S[redacted] B[redacted]. (hereinafter "S.B.") (See Chart 1 below)

d. Between February 26, 2022, and February 28, 2022, 47,059 USDT was then transferred from wallet TUg9 to wallet TKcU at the Binance exchange, which was identified by Binance as the deposit address for account in the name of S.B., user ID 36412394 (See Chart 1 below).

Chart 1


Summary of USDT (Tether) transactions
okcoin
OKCoin Exchange
492,159 USDT sent on 2/25/22
494,623 USDT sent on 2/25/22
182,654 USDT sent on 2/26/22
500,000 USDT sent on 2/26/22
tether
TWXd wallet
492,159 USDT sent on 2/25/22
tether
TPQ2 wallet
tether
TBAF wallet
tether
TTSq wallet
4 USDT transactions 720,000 total 2/26/22 - 2/28/22
12,658 USDT sent on 2/26/22
5 USDT transactions 47,000 total 2/26/22 - 2/28/22
BINANCE
Binance account
user ID: 362242577 (TG9M wallet)
BINANCE
Binance account
user ID: 63916663 (TNqo wallet)
tether
TUg9 wallet
5 USDT transactions 47,059 total 2/26/22 - 2/28/22
BINANCE
Binance account
user ID: 36412394 (TKcU wallet)

22. I provided Binance with my contact information if an account holder wished to speak about the investigation.

23. On March 25, 2022, S.B. sent me an email stating in summary that: (1) he is an Indian citizen; (2) he owns the Binance account with wallet TKcU (see paragraph 21(b) above); (3) all of the cryptocurrency he has bought was with his own "hard earned" money; and (4) he wants to help the investigation.

24. On March 26, 2022, at 8:48 a.m. MST, I received a phone call with a number originating from India. The male voice claimed to be S.B. and said all of his cryptocurrency transactions are from his own personal funds. S.B. also has friends he sends cryptocurrency to for short term loans to avoid banking regulations. S.B. said he is in the garment industry where his primary source of funds is the manufacturing of clothing. S.B. said that he moves money through various wallets because he doesn't trust exchanges and wants to be prepared in the event he is exposed to any risk of losing his funds. S.B. uses other exchanges such as BuyBit and KuCoin but denies ever having used the OK Coin exchange. S.B. said he uses the USDT token whenever he needs to send a certain kind of cryptocurrency because of its fast processing speed and for use with ERC20 tokens on the Ethereum blockchain. He denied any involvement in defrauding residents in the United States.

25. In the days following this initial telephonic interview, I received several emails and telephone calls from S.B. For example, on March 26, 2022, S.B. sent an email message claiming ownership of virtual wallet TUg9. This is the wallet that received approximately 47,000 USDT from TPQ2 originating from D.M. Later on March 26, 2022, S.B. sent an email

message making the following statements: (1) he controls wallet TUg9; (2) wallet TPQ2 belongs to his friend; (3) he borrowed the 47,000 USDT from his friend (TPQ2) because his "opened positions needed more margin;" (4) he explained his high trading volume by saying he has a "bad habit of overtrading. To keep myself away from overtrading I keep transferring funds from exchange to wallet so that I don't trade much;" and (5) "…I so far never did anything wrong to anyone."

26. On March 28, 2022, S.B. sent an email message stating the following: (1) he denied wrongdoing; (2) the funds sent to him from TPQ2 were returned to TPQ2 within two days; and (3) he told his friend who controls TPQ2 to contact me.

27. On April 6, 2022, I received a call from 91 [redacted] (India) from a male caller self-identified as G[redacted] S[redacted] (hereinafter "G.S."). G.S. claimed to be the owner of crypto wallet TPQ2iafQDsyVGMKsjV1MB8oN2 (referenced as TPQ2). G.S. got my number from S.B. who I previously spoke with by phone and email in reference to the transactions previously described above. G.S. admitted receiving the transactions for 494,623 USDT and 492,159 USDT on February 25, 2022. He explained that he received both deposits from another Indian man he met at a party in Dubai (Dubai John DOE). The party was an event he learned about through a cryptocurrency enthusiast group on the encrypted social media platform Telegram. G.S. claimed to not know the identity of Dubai John DOE but remembers what he looks like and would recognize him if he saw him again.

28. G.S. stated he obtained the cryptocurrency in exchange for software. He said that Dubai John DOE used a smart phone to scan G.S.'s crypto wallet QR code to make the transfer. Once G.S. confirmed receipt of the tokens, he provided Dubai John DOE a hard drive

containing the software. Dubai John DOE did not show any interest in software before G.S. offered it in exchange for the virtual currency. G.S. is unsure what Dubai John DOE plans to do with the software. G.S. does not know how to reach Dubai John DOE nor does he know his name. G.S. said that he has no way to confirm whether the funds are from legal sources or not.

29. G.S. said that he works in software development and also loans money to people for interest using cryptocurrency. He said he prefers conducting transactions using the USDT cryptocurrency token for its stability so that the value doesn't fluctuate in the transfer process. G.S. has known S.B. for many years and is concerned about his funds being frozen in his Binance account. G.S. believes S.B. has approximately $200,000 in cryptocurrency that he is unable to access. G.S. wants to cooperate with hopes of unfreezing those assets and to help his friend. S.B. has told G.S. that he is very upset about this.

30. G.S. said he sent me an email but I did not receive one from him. G.S. claimed a desire to cooperate and provide any documentation necessary. G.S. later called your affiant and said he had difficulty sending an email but provided his email as g[redacted]7799@gmail.com. G.S. refused to provide any identifying information to confirm his identity.

31. On April 11, 2022, I received an email from j[redacted]123456@gmail.com which matches the email address on the customer records provided by Binance for R.R. user ID 362242577. The email contained the following text:

> Dear Sir, I tried calling your number [redacted] but I was unable to reach you. Kindly guide me in resolving my account freeze.

32. On April 13, 2022, I responded to this message with the following content, and as of the date of this affidavit have not received a response:

> If I provide you a wallet address, would you please return the funds sent to you in these transactions totaling 720,000 USDT? As you may be aware, these tokens you received were stolen from a victim in the US. Once these funds are confirmed to be received by the US Government, we will request Binance unfreeze your account. If you choose not to return the funds, please let us know that too.

2022-02-28T16:08:36.000+00:00	f88626ea1094f5083cf6a3566226d70cffe7f37fb503369728e41873d45ff640	TG9MgfSWDKzjuxnbBvp2RwG7oGaCBGxtkV	(70,000.00)
2022-02-26T16:51:09.000+00:00	24ad5691d4803f6aaee311ff16d45a849870f5d283709b063040bcc2c87aa04e	TG9MgfSWDKzjuxnbBvp2RwG7oGaCBGxtkV	(150,000.00)
2022-02-26T09:19:12.000+00:00	554553f6344a50dc06a678c2422ae1e9f75829cdf3bea47923213f4bde6061b6	TG9MgfSWDKzjuxnbBvp2RwG7oGaCBGxtkV	(250,000.00)
2022-02-26T05:09:30.000+00:00	ae0ff11c286899020257ab53dc7f4378168aacb904eec618d66440f451104e7d	TG9MgfSWDKzjuxnbBvp2RwG7oGaCBGxtkV	(250,000.00)

On May 13, 2022, I wrote an email to R.S. from the email provided in the Binance account records in which I stated the following:

> Mr. [R.S.],
>
> The government of the United States has requested Binance to temporarily freeze your account pending a seizure warrant for the funds you received in the transaction listed below (12,658 USDT). These funds were stolen from a victim in the United States before they were sent to you. The funds are being seized so they can be returned to the victim. Any information you have about the person who controls the originating wallet would be useful information. Please let me know if you are interested in cooperating in this investigation.

Amount: 12658
BUSD: 12663.07
Deposit Address: TNqonJMEhRV5m6AFQXQbiekhyUHs94p1Q6
Source Address: TPQ2iafQDsyVGMKsjV1MB8oN2tjrKboMsq

TXID: d1b12f508c54aebaa7db3c0864365410299043db4fa6f061d1d67b2e6d60f01bCreate Time: 2/26/2022 19:04

33. I received the following email response 28 days later on June 10, 2022:

> Sir,
> I am utterly dismayed to discover that my Binance account has been freezed. This is to bring to your notice that on 02.04.2022 I purchased the funds amounting to 12,658 USTD from one unknown vendor and accordingly the said amount was transferred in my account. But I am completely unaware of this fact that the funds I have received were stolen before they were sent to me. I would like to inform you that I am a bonafide purchaser and I have no information about the vendor from whom I have received the funds since it was a random purchase of the funds from one random online vendor. I further submit that since it is a online transanction business and there are multiple vendors who have the Wallet address information therefore, being a bonafide purchaser of the funds I have no knowledge that the funds received from the vendor were stolen one from some other person. I have no objection if the seized amount is returned to the victim whosoever it is. Kindly take the needful action and verify the vendor who deposited the stolen money so that the matter can be resolved at the earliest and unfreeze the account so that no further harassment is faced.

CONCLUSION

35. Based on the foregoing, I believe there is probable cause that the Defendant Cryptocurrencies:

Binance user ID 36412394, in the name of S.B.:

Currency Name	Currency Code	Amount
USDT	TetherUS	46,990
USDT	TetherUS	63,850

Binance user ID 362242577, in the name of R.R.:

Currency Name	Currency Code	Amount
BNB	BNB	9.9990
BTTC	BitTorrent	319,112,718

SHIB	SHIBA INU	102,070,628.68
FTM	Fantom	1,253.602517
ETH	Ethereum	3.998335
USDT	TetherUS	145,400.1033
MTH	Monetha	305,871.433
DOGE	Dogecoin	45,838.48318

Binance user ID 63916663, in the name of R.S.:

Currency Name	Currency Code	Amount
BTC	Bitcoin	2.83040268
ETC	Ethereum Classic	77.72361915

were involved in a transaction or attempted transactions in violation of 18 U.S.C. §§ 1956 and 1957 (Money Laundering), and which constitute or were derived from proceeds traceable to violations of 18 U.S.C. §1343, and are therefore subject to forfeiture pursuant to 18 U.S.C. §§981(a)(1)(A) and (a)(1)(C).

I swear, under penalty of perjury, that the foregoing is true and correct.

Dan Grossenbach
Postal Inspector
U.S. Postal Inspection Service

Subscribed and sworn to before me this 24 day of October, 2022.

Notary Public

JAY WILBER
Notary Public - State of Arizona
PIMA COUNTY
Commission # 562169
Expires March 31, 2023